Guidelines by OHCSF

TABLE OF CONTENTS

Preamble

This Guideline is issued to: ensure accountability and productivity in the usage of all government Personal Information Technology Devices (hereafter referred to as PITeD); foster strict adherence to government policies and global best practice in respect of data protection; provide clarity on the legitimate uses required on the part of users and the consequences of breaching the provisions of the Guideline.

PART I: Scope of the Guideline

a) This Guideline shall apply to the usage of PITeD in Ministries, Departments and Agencies of the Federal Government.
b) This Guideline shall be applied harmoniously with internal regulatory framework on the provision and usage of PITeD (if any) by Ministries, Departments and Agencies of the Federal Government.

PART II: Definitions

The underlisted terms in this Guideline, are supplied for ease of reference. No term is intended to be read or used in any context outside the intendment of this Guideline.

a) "Department" means any unit charged with the responsibility to carry out any function with an MDA
b) "General Services Department" means any unit charged with responsibility of providing work-tools.
c) "general usage" means usage by more than one person in a department
d) "hot spot" means a channel for sharing internet service.
e) "Information", means , any information owned or used by MDAs, such as :
    i. any list of employees, customers, or clients
    ii. any database information, including addresses, emailaddresses and telephone numbers.
f) "issuing MDA" means the MDA that issues or allocates a PITeD to a user
g) "illegitimate purposes" means purposes that are prohibited by the issuing MDA, public policy or law.
h) "Supervising Officers" means any officer given responsibility to supervise general usage of PITeD.
i) "IT" means Information Technology.
j) "PITeD" means any piece of IT, devices purchased, leased or donated to Ministries, Department and Agencies (MDAs).
k) "users" means all employees, agents, contractors, consultants and business partners who have access to government's information and information systems and who are allocated PITeD as work-tools.

PART III: Objectives

The objectives of this Guideline are as follows:

a) To ensure accountability and productivity in the usage of all government PITeD,

b) To promote an orderly process of digitalization with a view to accelerating sustainable development of digital economy in Nigeria.

c) To foster strict adherence to government policies and global best practice in respect of the protection of data which are being processed through the usage of PITeD,

d) To promote trust in the provision and usage of PITeD in the delivery of public services.

e) To provide clarity on the legitimate uses required on the part of users.

f) To prescribe disciplinary consequences for unauthorized use of PITeD.

Part IV: Types and Sources of Personal Information Technology Device (PITeD)

A) The types of PITeD referred to in this Guideline are:

i. Laptops,
ii. E-pads (otherwise known as tablets),
iii. Mobile Phones,
iv. Desktop Personal Computer,
v. All-in-one Personal Computers, and
vi. Printers/copiers

B) The sources of PITeD referred to in this Guideline are by:

i. Appropriation,
ii. Lease,
iii. Donation,
iv. Public Private Partnership (PPP), and
v. Any other legitimate source.

Part V: Operative Principles on the Usage of PITeD

a) Users shall not use PITeD for any illegitimate purposes; accordingly each MDA shall immediately, after the issuance of this Guideline, determine what constitute legitimate usage in the light of its mandate and bring same to the attention of users.

b) Generally, a user shall not subject PITeD to any usage that may cause:

i. Damage or liability to the issuing MDA
ii. Injury to any person or property
iii. Breach of cyber-security
iv. Breach of data privacy
v. Damage to the PITeD or any Information Security Infrastructure particularly as a result of using the internet, downloading viruses or harmful cookies or harmful softwares – whether advertently or inadvertently.
vi. Loss of official government data
vii. Compromise of data integrity
viii. Abridgment or derogation of fundamental rights and freedoms.

c) Any usage that is unlawful for any government asset shall be unlawful in the use of PITeD, accordingly, a user shall, in addition to the foregoing provisions, be guided by the provisions of **Schedule A** of this Guideline.

Part VI: Operative Principles in Respect of the Provision PITeD

a) In the light of the digitalization initiatives of government, every officer is eligible to use PITeD, subject to availability of resources; accordingly individual MDAs shall deliberately promote fair allocation of PITeD to their respective officers.

b) Agents, contractors, consultants and business partners are eligible to PITeD as may be necessary for the execution of the Terms of Reference (TOR) as contained in their engagements with Government.

c) Each PITeD issued to a user shall remain the property of the issuing MDA until the ownership of such device has been duly transferred by the issuing MDA.

d) Individual MDAs shall use Service Level Agreements that are in consonance with the standards approved by National Information Technology Development Agency (NITDA) to ensure sustainability of PITeD usage in the delivery of public services.

Part VII: Creation of PITeD Register/Database

a) Upon acquisition of PITeD by an MDA, the department or unit responsible for Information Communication Technology (ICT) in such MDA shall register the acquired devices in a PITeD database.

b) In order to manage the register accurately and efficiently:

i. Each PITeD shall be tagged with a permanent and unique asset tag mapped to the serial number of the item, as a means of identification of the PITeD by the issuing MDA.
ii. The information registered against each PITeD shall include but not limited to the following:

a) Serial Number

b) Location

c) Type of asset

d) Owner

e) Department

f) User's job role

Part VIII: Responsibilities of Users

a) Except as otherwise permitted, users shall not remove PITeD from the premises of the issuing MDA.

b) In the event of loss or theft of a PITeD, the concerned user shall immediately report the occurrence of the loss or theft to the ICT and General Services Departments of the issuing MDA.

c) In the event of loss or theft of a PITeD, the concerned user shall make a formal complaint to the Nigeria Police and obtain a police report which report shall be filed with the issuing MDA.

d) A user shall return the PITeD issued to him in line with the conditions stipulated by the issuing MDA; accordingly, each MDA shall upon the issuance of this Guideline, set forth the conditions (if not in existence) under which a user shall return PITeD.

e) Where a user (who is a civil servant) is exiting the Service (or being redeployed), he must return the PITeD to the General Services Department after its condition has been certified by the ICT department.

f) Where a user (who is a consultant, contractor, agent or partner) has concluded his assignment/consultancy with the MDA, he must return the PITeD to the General Service Department after its condition has been certified by the ICT department.

g) Notwithstanding anything to the contrary in this Guideline, a user who has already been duly issued PITeD prior to the issuance of this Guideline shall not be denied the usage of such PITeD only for the reason that the conditions for its usage or return have not been issued by the issuing MDA.

h) A user shall be accountable for all his acts and omissions in the usage of the PITeD issued to him and where negligence or criminal conduct is established, he shall be liable in accordance with applicable law or regulatory instruments.

i) A user may change his password as frequently as necessary after receiving or being allocated a PITeD, provided that the issuing MDA

may cause the password to be changed at any time with or without the knowledge of the user.

j) User should note that the ICT Department may access the PITeD in his absence.

k) Any person, who by conduct or omission, contravenes the provisions of this Guideline shall be liable to disciplinary action in accordance with extant rules and regulations in the respective MDA.

Part IX: Responsibilities of Supervising Officers

a) A supervising officer who has been given responsibility over PITeD for general usage by his department shall give periodic report on the condition of the PITeD to the issuing MDA through the ICT department.

b) The issuing MDA shall provide a schedule which shall be used for reports on PITeD by the concerned supervising officers.

c) Regardless of any schedule by the issuing MDA, a supervising officer who has been given responsibility over PITeD for general usage by his department shall create a log in which he shall:

   i. on monthly basis, record the functionality of PITeD under his supervision;

   ii. report any adverse occurrence such as loss, damage or theft;

d) Supervising officers shall also ensure compliance with the provisions of this Guideline.

Part X: Data Privacy and Protection.

a) Each MDA shall ensure that the usage of PITeD is consistent with Nigeria Data Protection Regulation and any regulatory instrument on data privacy and protection in Nigeria.
b) The measures to be taken by each MDA for the purpose of data protection and accountability shall include but not limited to the following:
   i. Designation or appointment of a suitable officer within the MDA as a Data Protection Officer (DPO).
   ii. Development of a Data Protection Policy in line with Nigeria Data Protection Regulation (NDPR) and other applicable regulatory instruments on data privacy and protection.

iii. Forwarding of the contact details of the data protection officer to the Office of the Head of Service and the Nigeria Data Protection Bureau.

c) In addition to the internal data protection policies, each MDA shall ensure information security in line with the following measures:

i. Only genuine applications, software and devices by MDAs can be used for official businesses.
ii. Forestall any compromise of its network and database by preventing access by unauthorized devices and users.
iii. Only Wi-fi (or Ethernet) permitted by the MDA can be connected to PITeD.
iv. PITeD should have up-to-date antivirus with endpoint detection and response system.
v. Access to file sharing or email sites or services other than that of the Government should be blocked.
vi. USB ports on the systems or laptops should be disabled.
vii. Only IT staff with Administrator privileges should install applications on the PITeD and this should be tracked and monitored in line with Schedule B of this Guideline.
viii. All applications installed on the laptops should be properly updated.
ix. Official information should not be stored on devices without MDA security controls.
x. All official request for software should be made through the ICT Department.

Part XI: Implementation Mechanism

a) The Permanent Secretary, Special Duties Office at the Office of the Head of the Civil Service of the Federation (or any other officer delegated by him) shall be responsible for monitoring compliance of MDAs with the provisions of this Guideline.
b) The function of such officers shall be as follows:
    i. Providing information on the operations of this Guideline.
    ii. Issuing notices of compliance in the case of breach or potential breach.
    iii. Investigating breaches of this Guideline and reporting findings to the Head of the Civil Service of the Federationfor appropriate actions.
    iv. Coordinating service-wide awareness and capacity building programmes subject to internal mechanisms for such programmes by MDAs
    v. Collaboration with relevant regulatory agencies towards the realization of the objectives of this Guideline
    vi. Enlisting the support of relevant indigenous and international organizations towards the realization of the objectives of this Guideline
    vii. Doing such other things that are necessarily incidental to the

attainment of the objectives of this Guideline.

Part XII: Miscellaneous

a) All government employees must maintain their work environment in an orderly manner and follow all rules to ensure proper use and maintenance.

b) Users must immediately report breach of any provision of this Guideline to their departmental head and/or to the ICT department, and comply with official procedures when a breach of the provision is suspected or reported.

c) Users should be aware that they can use whistle blowing and raising a concern if it is believed that someone is misusingofficial information or electronic equipment.

d) It is the users' responsibility to undertake education and seek awareness on security and using MDA information and technology, including e-learning, in order to understand, recognize, and report threats, risks and incidents.

e) In the event that any PITeD develops a fault, the ICT Department should be immediately contacted for its repair or otherwise. On no account should any staff engage the services of private technician(s) to fix any fault on any PITeD.

f) All requests to use software not currently approved by MDA must be subject to the Software Approvals process though the ICT Department.

SCHEDULES TO THIS GUIDELINE

Schedule A: Communications (Emails, Websites, Social Media, Voice)

a) Each user is under strict obligation to use descent words in all communications.
b) Transmission of unsolicited emails(SPAM) is prohibited.
c) It is unlawful to alter the information of another person without consent or legal basis.
d) No user should misrepresent his own identity particularly by pretending to be whom he is not.
e) Each user is expected to be conversant with mails that are likely to be fraudulent and to avoid engaging with such mails in any way.
f) Using official mail for personal purposes is not permitted.
g) It is unlawful to visit online platforms that operate in violation of public policy. Examples sites that promote pornography, cultism, terrorism, hate, slavery, etc. A user may give information on such websites that should be blocked by MDAs.
h) It is unlawful to access, share or process any information or personal data on any platform without authorization that is duly granted in line with extant data protection framework.

Schedule B: Monitoring of Network Communications and PITeD Usage

a) MDAs shall take appropriate measures to block or restrict access to unsafe online platforms as a part of prudent measures necessary for the security of its network.
b) Monitoring activities shall have regard for privacy rights and in no way should a user be overreached in his private space.
c) MDAs reserve the right to monitor, at any time, any communication that use their networks in any way, including data, voice mail, telephone logs, internet use and network traffic.
d) MDAs may review network communications activity and may analyze usage data appropriately. Analyzed data may be published as occasions may warrant.
e) It is unlawful to disable or uninstall any software or hardware in PITeD.
f) An issuing MDA may, with or without notice, investigate the usage of PITeD by any user.
g) Any information or data saved in PITeD shall be presumed to be official, accordingly a user shall not prevent inspection of PITeD by the issuing MDA on the grounds of privacy or any other legal claim.